

§ 33 Finite fields

What kind of finite sets can be fields?
Can we classify them?

Observation 1: If F is a finite field,
there is a prime number n s.t. $\mathbb{Z}_n \subset F$
field ext.

Why: take the mult. identity $1 \in F$

consider the elements $0, 1, 2 = 1+1, \dots, k = \underbrace{1+\dots+1}_{k \text{ times}}, \dots$

since F is finite, we come back to 0

at a certain step. $\rightarrow \mathbb{Z}_n \subset F$

We say F is of characteristic n for such n

Observation 2 (Thm 33.1) If F is a finite field with q elements, $E \supset F$ is an extension of degree k , then E has q^k elements

Why E has a basis $\alpha_1, \dots, \alpha_k$ over F

$\rightarrow$ elements of E are $\sum_{i=1}^k \beta_i \alpha_i$ $\beta_i \in F$

possibilities of $(\beta_i)_{i=1}^k$: q^k in total

$\rightarrow$ Cor 33.2 If F is a finite field, it has p^n elements for some prime p , int n

In fact, up to isomorphism, there is a unique field with p^n elements. We call it $GF(p^n)$
Galois field

Ex. $GF(p) = \mathbb{Z}_p$

$GF(4) = \mathbb{Z}_2(\alpha \mid \alpha^2 + \alpha + 1 = 0)$

$GF(9) = \mathbb{Z}_3(\beta \mid \beta^2 + 1 = 0)$

• How to find $GF(p^n)$ (existence)

find a polynomial $f(X) \in \mathbb{Z}_p[X]$ with

• degree p^n

• p^n distinct roots (no ^{roots with} multiplicity), which form a field

• How to get $E \cong GF(p^n)$ from $|E| = p^n$ (uniqueness)

show that same polynomial $f(X)$ as above

would work for E : $f(X) = \prod_{\alpha \in E} (X - \alpha)$

Observation 3 If E is a finite field, its multiplicative group $E^\times = \{\alpha \in E \mid \alpha \neq 0\}$ is a cyclic group (Cor 23.6)

Why: $E^\times$ is a finite comm. group, hence isomorphic to $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ (April 1; Thm 11.12)

We have $\begin{cases} |E^\times| = n_1 \dots n_k \\ \alpha^m = 1 \text{ for } m = \text{lcm}(n_1, \dots, n_k) \end{cases}$
least common mult.

Then $X^m - 1$ would have any $\beta \in E$ as its

root: $\beta^m - 1 = 0 \Rightarrow X^m - 1 = \prod_{\alpha \in E^\times} (X - \alpha)$

$\Rightarrow m = |E^\times| \Rightarrow n_1 \dots n_k = m = \text{lcm}(n_1, \dots, n_k)$

$\Rightarrow \gcd(n_1, \dots, n_k) = 1 \Rightarrow \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k} \cong \mathbb{Z}_{n_1 \dots n_k}$
Cor 11.6

Now we know $X^{p^n-1} - 1 = \prod_{\alpha \in E^\times} (X - \alpha)$ if $|E| = p^n$

so $X^{p^n} - X = \prod_{\alpha \in E} (X - \alpha)$ with an extra $X - 0 = X$

This is the candidate for $f(X)$ corresp. to $GF(p^n)$

If we fix an algebraically closed field $K \supset \mathbb{Z}_p$

we can talk about the roots for $f(X) = X^{p^n} - X$

in $K \Rightarrow$ are they distinct? do they form a field?

Lem. 33.8 $X^{p^n} - X$ has p^n dist. roots in K

Proof. Differentiation gives

$$X^{p^n} - X = \prod_{i=1}^{p^n} (X - \alpha_i) \leadsto p^n X^{p^n-1} - 1 = \sum_{i=1}^{p^n} \prod_{j \neq i} (X - \alpha_j)$$

If there is a repetition in $(\alpha_i)_{i=1}^{p^n}$

$X^{p^n} - X$ and $p^n X^{p^n-1} - 1$ would have a common root.

But $p^n = 0$ in $K \supset \mathbb{Z}_p$ $\square$

Lem 33.9 $(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$ in K

Proof Binomial expansion formula and

p divides $\binom{p}{k}$ for $0 < k < p$

$$\rightarrow (\alpha + \beta)^p = \alpha^p + \beta^p \text{ in } K \supset \mathbb{Z}_p.$$

Use induction to get the claim $\square$

Cor. $\{\alpha \in K \mid \alpha^{p^n} = \alpha\}$ forms a field.

Proof Lem 33.9 says this is closed under $+$

Compat. with prod. is $(\alpha\beta)^{p^n} = \alpha^{p^n} \beta^{p^n}$

$\rightarrow$ subring of K .

Compat with inverse: $(\frac{1}{\alpha})^{p^n} = \frac{1}{\alpha^{p^n}}$

1. The first part of the paper is devoted to the study of the

properties of the function $f(x)$ defined by the equation

$$f(x) = \int_0^x \frac{1}{1+t^2} dt$$

It is well known that this function is increasing and concave

downwards. The first part of the paper is devoted to the study of the

properties of the function $f(x)$ defined by the equation

$$f(x) = \int_0^x \frac{1}{1+t^2} dt$$

It is well known that this function is increasing and concave

downwards. The first part of the paper is devoted to the study of the

properties of the function $f(x)$ defined by the equation

$$f(x) = \int_0^x \frac{1}{1+t^2} dt$$

It is well known that this function is increasing and concave

downwards. The first part of the paper is devoted to the study of the

properties of the function $f(x)$ defined by the equation

$$f(x) = \int_0^x \frac{1}{1+t^2} dt$$

It is well known that this function is increasing and concave

downwards. The first part of the paper is devoted to the study of the

properties of the function $f(x)$ defined by the equation

$$f(x) = \int_0^x \frac{1}{1+t^2} dt$$

It is well known that this function is increasing and concave

downwards. The first part of the paper is devoted to the study of the

properties of the function $f(x)$ defined by the equation

It is well known that this function is increasing and concave

downwards. The first part of the paper is devoted to the study of the

properties of the function $f(x)$ defined by the equation

It is well known that this function is increasing and concave

downwards. The first part of the paper is devoted to the study of the

properties of the function $f(x)$ defined by the equation

It is well known that this function is increasing and concave

downwards. The first part of the paper is devoted to the study of the